According to a new market research report titled, **“AI in Cybersecurity Market by Technology (ML, NLP), Security (Endpoint, Cloud, Network), Application (DLP, UTM, IAM, Antivirus, IDP), Industry (Retail, Government, BFSI, IT, Healthcare), and Geography - Global Forecasts to 2029,”** the global artificial intelligence in cybersecurity market is expected to grow at a CAGR of 24.2% during the forecast period to reach $66.22 billion by 2029.

Download Free Sample Report Now

The increasing demand for advanced cybersecurity solutions and privacy, the growing significance of AI-based cybersecurity solutions in the banking sector, the rising frequency and complexity of cyber threats are the key factors driving the growth of the artificial intelligence in cybersecurity market. In addition, the growing need for AI-based cybersecurity solutions among small and medium-sized enterprises (SMEs) are creating new growth opportunities for vendors in the AI in cybersecurity market.

However, the lack of skilled AI professionals, the perception of AI in cybersecurity as an uncomprehensive security solution, and the impacts of the COVID-19 pandemic are expected to restrain the growth of this market to a notable extent.

The global artificial intelligence in cybersecurity market is segmented based on components (hardware, software, services), technology (machine learning, natural language processing, context-aware computing), security (application security, endpoint security, cloud security, network security), by applications (data loss prevention, unified threat management, encryption, identity & access management, risk & compliance management, antivirus/antimalware, intrusion detection/prevention system, distributed denial of service mitigation, security information & event management, threat intelligence, fraud detection), by deployment (on-premises, cloud-based), industry vertical (retail, government & defense, automotive & transportation, BFSI, manufacturing, infrastructure, IT & telecommunication, healthcare, aerospace, education, energy). The study also evaluates industry competitors and analyses the market at the country level.

Based on component, the AI in cybersecurity market is segmented into software, hardware, and services. In 2022, the software segment is estimated to account for the largest share of the artificial intelligence in cybersecurity market. The larger share and highest CAGR of this segment is primarily driven by the growing data security concerns, the increase in demand for AI platforms solutions for security operations, the surge in demand for robust and cost-effective security solutions among business enterprises to strengthen their cybersecurity infrastructure.

Speak to our Analysts to Understand the Impact of COVID-19 on Your Business

Based on technology, the market is segmented into machine learning, natural language processing (NLP), and context-aware computing. In 2022, the machine learning technology segment is estimated to account for the largest share of the artificial intelligence in cybersecurity market. The large share and highest CAGR of this segment is primarily attributed to its advanced ability to collect, process, and handle big data from different sources that offer rapid analysis and prediction. It also helps analyze user behavior and learn from them to help prevent attacks and respond to changing behavior. In addition, it helps find threats and respond to active attacks in real-time, reduces the amount of time spent on routine tasks, and enables organizations to use their resources more strategically, further supporting the growth of the machine learning technology market in the coming years.

Based on security, the market is segmented into network security, cloud security, endpoint security, and application security. In 2022, the network security segment is estimated to account for the largest share of the artificial intelligence in cybersecurity market. The large share of this segment is attributed to the adoption of the Bring Your Own Device (BYOD) trend, the increasing number of APTs, malware, and phishing attacks, the increasing need for secure data transmission, the growing demand for network security solutions, and rising privacy concerns. However, the cloud security segment is slated to register the highest CAGR during the forecast period due to the increased adoption of Internet of Things (IoT) devices, surge in the deployment of cloud solutions, the emergence of remote work and collaboration, the increasing demand for robust and cost-effective security services.

Based on application, this market is segmented into data loss prevention, unified threat management, encryption, identity & access management, risk & compliance management, intrusion detection/prevention system, antivirus/antimalware, distributed denial of service (DDoS) mitigation, Security Information and event management (SIEM), threat intelligence, and fraud detection. In 2022, the identity and access management segment is estimated to account for the largest share of the artificial intelligence in cybersecurity market. The large share of this segment is attributed to the increase in security concerns among organizations, the increasing number and complexity of cyber-attacks, the growing need for integrity & safety of confidential information in industry verticals, and the growing emphasis on compliance management. However, the data loss prevention segment is slated to register the highest CAGR during the forecast period due to the increasing regulatory and compliance requirements and the growing need to address data-related threats, including the risks of accidental data loss and exposure of sensitive data in organizations.

Quick Buy – "Artificial Intelligence in Cybersecurity Market by Technology (ML, NLP), Security (Endpoint, Cloud, Network), Application (DLP, UTM, IAM, Antivirus, IDP), Industry (Retail, Government, BFSI, IT, Healthcare), and Region - Global Forecasts to 2029"

Based on industry vertical, the market is segmented into government & defense, retail, manufacturing, banking, financial services, and insurance (BFSI), automotive & transportation, healthcare, IT & telecommunication, aerospace, education, and energy. In 2022, the IT & telecommunication sector is estimated to account for the largest share of the AI in cybersecurity market. The large share of this segment is mainly attributed to increasing incidence of security breaches by cybercriminal, shifting preference from traditional business models to sophisticated technologies, and including IoT devices, 5G, and cloud computing. However, the healthcare sector is slated to register the highest CAGR during the forecast period due to the rising sophistication levels of cyber-attacks, the growing incorporation of advanced cybersecurity solutions, the exponential rise in healthcare data breaches, and the growing adoption of IoT & connected devices across the healthcare sector.

Based on deployment, the market is segmented into on-premises and cloud-based. In 2022, the on-premises segment is estimated to account for the largest share of the artificial intelligence in cybersecurity market. The large share of this segment is attributed to the increasing necessity for enhancing the internal processes & systems, security issues related to cloud-based deployments, and the rising demand for advanced security application software among industry verticals. However, the cloud-based segment is slated to register the highest CAGR during the forecast period due to the increasing number of large enterprises using cloud platforms for data repositories and the growing demand to reduce the capital investment required to implement cybersecurity solutions. In addition, several organizations are moving operations to the cloud, leading cybersecurity vendors to develop cloud-based solutions.

Based on geography, in 2022, North America is estimated to account for the largest share of the overall artificial intelligence in cybersecurity market. The large market share of North America is attributed to the presence of major players along with several emerging startups in the region, the increase in government initiatives towards advanced technologies, such as artificial intelligence, the proliferation of cloud-based solutions, the increasing sophistication in cyber-attacks, and the emergence of disruptive digital technologies. However, Asia-Pacific is expected to register the highest CAGR during the forecast period. Factors such as the rising number of connected devices, the increasing privacy &

security concerns, the growing awareness regarding cybersecurity among organizations, rapid economic development, high adoption of advanced technologies, such as IoT, 5G technology, and cloud computing are contributing to the growth of this market in Asia-Pacific.

The report also includes an extensive assessment of the key strategic developments adopted by the leading market participants in the industry over the past four years (2019–2022). The artificial intelligence in cybersecurity market has witnessed several partnerships & agreements in recent years that enabled companies to broaden their product portfolios, advance the capabilities of existing products, and gain cost leadership in the cybersecurity market. For instance, in 2021, Juniper Networks, Inc. (U.S.) launched Juniper Cloud Workload Protection, a software designed to automatically defend application workloads in any cloud or on-premises data center environment against application exploits in real-time. Similarly, in 2021, SecurityBridge (Germany) partnered with Fortinet, Inc. (U.S.) to address the security challenges posed by vulnerabilities within the SAP landscape. Also, in 2021, Check Point Software Technologies Ltd. (Israel) launched security gateways to protect SMBs against threats.

The global artificial intelligence in cybersecurity market is fragmented in nature. The major players operating in this market are Amazon Web Services, Inc. (U.S.), IBM Corporation (U.S.), Intel Corporation (U.S.), Microsoft Corporation (U.S.), Nvidia Corporation (U.S.), FireEye, Inc. (U.S.), Palo Alto Networks, Inc. (U.S.), Juniper Networks, Inc. (U.S.), Fortinet, Inc. (U.S.), Cisco Systems, Inc. (U.S.), Micron Technology, Inc. (U.S.), Check Point Software Technologies Ltd. (U.S.), Imperva (U.S.), McAfee LLC (U.S.), LogRhythm, Inc. (U.S.), Sophos Ltd. (U.S.), NortonLifeLock Inc. (U.S.), and Crowdstrike Holdings, Inc. (U.S.).

Scope of the Report:

AI in Cybersecurity Market by Component

- Hardware
  - Processors
  - Networking Solutions
  - Memory Solutions
- Software
  - AI Platforms
  - AI Solutions
- Services
  - Deployment & Integration

  - Support & Maintenance

AI in Cybersecurity Market by Technology

- Machine Learning
- Natural Language Processing
- Context-aware Computing

AI in Cybersecurity Market by Security Type

- Application Security
- Endpoint Security
- Cloud Security
- Network Security

AI in Cybersecurity Market by Application

- Data Loss Prevention
- Unified Threat Management
- Encryption
- Identity and Access Management
- Risk and Compliance Management
- Antivirus/Antimalware
- Intrusion Detection/Prevention System
- Distributed Denial of Service (DDoS) Mitigation
- Security Information and Event Management (SIEM)
- Threat Intelligence
- Fraud Detection

AI in Cybersecurity Market by Deployment Type

- On-premises
- Cloud-based

AI in Cybersecurity Market by Industry Vertical

- Retail
- Government & Defense

- Automotive & Transportation
- BFSI
- Manufacturing
- Infrastructure
- IT & Telecommunication
- Healthcare
- Aerospace
- Education
- Energy

AI in Cybersecurity Market by Geography:

- North America
    - U.S.
    - Canada
- Europe
    - Germany
    - U.K.
    - France
    - Italy
    - Spain
    - Rest of Europe
- Asia-Pacific
    - Japan
    - China
    - India
    - South Korea
    - Rest of Asia-Pacific
- Latin America
    - Mexico

    - Brazil
    - Rest of Latin America
- Middle East & Africa